What is claimed is:

1. A contactless communication tag that is attached to a product and provides product information, the contactless communication tag comprising:

a contactless communication unit, which wirelessly exchanges data with a tag reader, creates a power source from a power signal received from the tag reader, and supplies the power source;

a storing unit in which the product information and encryption key related information are stored; and

an encryption unit, which encrypts the product information to be transmitted to the tag reader based on the encryption key related information.

2. The contactless communication tag of claim 1, wherein the encryption key related information includes an encryption key for encryption of the product information and encryption key index information indicating a storing location of the encryption key in a storing means included in the tag reader; and

the encryption unit provides the encryption key index information corresponding to the encryption key in response to an encryption key specifying request message received from the tag reader.

3. The contactless communication tag of claim 1, wherein the encryption key related information includes a seed value for creation of the encryption key and seed value index information indicating a storing location of the seed value in a storing means included in the tag reader; and

the encryption unit provides the seed value index information to the tag reader to an encryption key specifying request message received from the tag reader.

4. The contactless communication tag of claim 1, wherein the encryption key related information includes a plurality of encryption keys and encryption key index information indicating storing locations of the plurality of encryption keys in a storing means included in the tag reader; and

the encryption unit provides the encryption key index information corresponding to an encryption key selected from the plurality of encryption keys in response to an encryption key specifying request message received from the tag

reader.

5. The contactless communication tag of claim 4, wherein the encryption unit provides the product information to the tag reader after encrypting the product information using the selected encryption key.

6. The contactless communication tag of claim 4, wherein the plurality of encryption keys is classified and assigned according to a classification reference including at least one of a type of industry, a manufacturer, a brand, and a product name; and

the encryption unit sequentially selects an encryption key from the plurality of encryption keys.

7. The contactless communication tag of claim 1, wherein the encryption key related information includes a plurality of seed values for creation of an encryption key and seed value index information indicating storing locations of the plurality of seed values in a storing means included in the tag reader; and

the encryption unit provides seed value index information corresponding to a seed value selected from the plurality of seed values in response to an encryption key specifying request message received from the tag reader.

8. The contactless communication tag of claim 7, wherein the encryption unit provides the product information to the tag reader after encrypting the product information using an encryption key created based on the selected seed value.

9. The contactless communication tag of claim 7, wherein the plurality of seed values is classified and assigned according to a classification reference including at least one of a type of industry, a manufacturer, a brand, and a product name; and

the encryption unit sequentially selects a seed value among the plurality of seed values.

10. The contactless communication tag of claim 1, further comprising a leaked encryption key updating unit, which transmits update request information that

requests discarding of an encryption key leaked through the contactless communication unit and updating into a newly assigned encryption key to the tag reader.

11. The contactless communication tag of claim 1, wherein the storing unit includes non-volatile memory, and further comprising a refresh processing unit that reads the product information from the storing unit and re-records the read product information on the storing unit.

12. The contactless communication tag of claim 1, further comprising a replay attack blocking unit which generates a one-time use random number, adds the one-time use random number to information to be transmitted to the tag reader, provides the information to the encryption unit, checks if a random number extracted from information received from the tag reader is the same as the one-time use random number, thereby blocking replay attack.

13. The contactless communication tag of claim 1, further comprising a covering unit that is separably attached to a tag exposed surface and blocks reading by the tag reader.

14. The contactless communication tag of claim 1, further comprising a decrypting unit that decrypts data received from the tag reader based on the encryption key related information.

15. The contactless communication tag of claim 1, wherein the contactless communication tag is destroyed not to be accessed by the tag reader when the product is unsealed or the contactless communication tag is detached from the product by an external force.

16. A contactless communication tag that is attached to a product and provides product information, the contactless communication tag comprising:

a contactless communication unit, which wirelessly exchanges data with a tag reader, creates a power source from a power signal received from the tag reader, and

supplies the power source;

a storing unit in which the product information, encryption key related information, and the number of times the product information is read by the tag reader;

an encryption unit, which encrypts the product information to be transmitted to the tag reader based on the encryption key related information; and

an information providing unit, which reads the product information stored in the storing unit in response to a product information request message received from the tag reader, provides the read product information to the encryption unit, and rejects provision of the product information if the number of times the product information is read exceeds a predetermined reference value.

17. The contactless communication tag of claim 16, further comprising a post management processing unit, which reads the product information stored in the storing unit and reading details even when the number of times stored in the storing unit exceeds the predetermined reference value and provides the product information and the reading details to a manager reader, if the post management processing unit receives a management information request message from the manager reader.

18. The contactless communication tag of claim 16, wherein the information providing unit creates date and time of reading and reading detail information including a serial number of a tag reader that transmits the product information request message every time of reading and stores the created information in the storing unit.

19. The contactless communication tag of claim 18, wherein the information providing unit reads the reading detail information stored in the storing unit in response to a reading detail information request message received from the tag reader and provides the read reading detail information to the tag reader.

20. The contactless communication tag of claim 16, further comprising a leaked encryption key updating unit that transmits update request information that requests discarding of an encryption key leaked through the contactless communication unit and updating into a newly assigned encryption key to the tag reader.

21. The contactless communication tag of claim 16, wherein the storing unit includes non-volatile memory, and further comprising a refresh processing unit that reads the product information from the storing unit and re-records the read product information on the storing unit.

22. The contactless communication tag of claim 16, further comprising a replay attack blocking unit which generates a one-time use random number, adds the one-time use random number to information to be transmitted to the tag reader, provides the information to the encryption unit, checks if a random number extracted from information received from the tag reader is the same as the one-time use random number, thereby blocking replay attack.

23. The contactless communication tag of claim 16, further comprising a covering unit that is separably attached to a tag exposed surface and blocks reading by the tag reader.

24. The contactless communication tag of claim 16, wherein the contactless communication tag is destroyed not to be accessed by the tag reader when the product is unsealed or the contactless communication tag is detached from the product by an external force.

25. The contactless communication tag of claim 16, wherein the encryption key related information includes an encryption key for encryption of the product information and encryption key index information indicating a storing location of the encryption key in a storing means included in the tag reader; and

the encryption unit provides the encryption key index information corresponding to the encryption key in response to an encryption key specifying request message received from the tag reader.

26. The contactless communication tag of claim 16, wherein the encryption key related information includes a seed value for creation of the encryption key and seed value index information indicating a storing location of the seed value in a storing

means included in the tag reader; and

the encryption unit provides the seed value index information to the tag reader to an encryption key specifying request message received from the tag reader.

27. A portable tag reader that reads information received from a contactless communication tag, the portable tag reader comprising:

a wireless communication unit, which wirelessly exchange data with the contactless communication tag and wirelessly sends a power required for the contactless communication tag;

a storing unit in which at least one encryption key related information is stored;

a decryption unit, which decrypts data received from the contactless communication tag based on encryption key related information that is selected from the encryption key related information by encryption key specifying information received from the contactless communication tag;

an information reading unit, which requests product information to the contactless communication tag attached to a product and reads the product information received from the contactless communication tag; and

an output unit, which outputs the read product information.

28. The portable tag reader of claim 27, wherein the encryption key related information includes at least one encryption key and the decryption unit decrypts product information received from the contactless communication tag by an encryption key selected based on the encryption key specifying information received from the contactless communication tag.

29. The portable tag reader of claim 27, further comprising a leaked encryption key updating unit that upon receipt of encryption key update request information concerning a leaked encryption key from the contactless communication tag, discards an encryption key designated by the encryption key update request information from the storing unit and updates with a newly assigned encryption key.

30. The portable tag reader of claim 27, wherein the encryption key related information includes a plurality of encryption keys that is classified and assigned

according to a classification reference including at least one of a type of industry, a manufacturer, a brand, and a product name; and

the decryption unit decrypts the product information received from the contactless communication tag using an encryption key selected from the plurality of encryption keys based on the encryption key specifying information received from the contactless communication tag.

31. The portable tag reader of claim 27, wherein the encryption key related information includes at least one seed value for creation of different encryption keys; and

the decryption unit decrypts the product information received from the contactless communication tag using an encryption key using a seed value selected based on the encryption key specifying information received from the contactless communication tag.

32. The portable tag reader of claim 31, further comprising a leaked seed value updating unit that, upon receipt of seed value update request information concerning a leaked seed value from the contactless communication tag, removes a seed value designated by the seed value update request information from the storing unit and updates with a newly assigned seed value.

33. The portable tag reader of claim 27, wherein the encryption key related information includes a plurality of seed values that is classified and assigned according to a classification reference including at least one of a type of industry, a manufacturer, a brand, and a product name; and

the decryption unit decrypts the product information received from the contactless communication tag using an encryption key created based on a seed value selected from the plurality of seed values based on the encryption key specifying information received from the contactless communication tag.

34. The portable tag reader of claim 27, further comprising a leaked encryption key updating unit that, upon receipt of update request information concerning leaked encryption key related information from the contactless communication tag, removes encryption key related information designated by the

update request information from the storing unit and updates with newly assigned encryption related information.

35. The portable tag reader of claim 27, further comprising a replay attack blocking unit which generates a one-time use random number, adds the one-time use random number to information to be transmitted to the tag reader, provides the information to the decryption unit, and checks if a random number extracted from information received from the tag reader is the same as the one-time use random number, thereby blocking replay attack.

36. The portable tag reader of claim 27, wherein the storing unit includes non-volatile memory, and further comprising a refresh processing unit that reads the product information from the storing unit and re-records the read product information on the storing unit.

37. The portable tag reader of claim 27, wherein a radio frequency (RF) circuit, the information reading unit, the decryption unit, and the storing unit of the wireless communication unit are implemented as application specific integrated circuit (ASIC).

38. The portable tag reader of claim 27, wherein the information reading unit specifies a plurality of product information from a type of industry, a manufacturer, a brand, and a product name based on the encryption key specifying information received from the contactless communication tag and provides the specified plurality of product information to the output unit, and the output unit outputs the specified plurality of product information.

39. The portable tag reader of claim 27, further comprising a reader authentication unit that authenticates an external portable tag reader by communicating with the external portable tag reader and outputs a result of authentication concerning the external portable tag reader to the output unit.

40. The portable tag reader of claim 27, wherein the output unit outputs a

result of reading of the product information through 7-segment display.

41. The portable tag reader of claim 27, wherein the output unit outputs a result of reading of the product information through a plurality of light emitting diodes having different colors.

42. The portable tag reader of claim 27, wherein the output unit outputs a result of reading of the product information through different beep sounds or voices.

43. The portable tag reader of claim 27, wherein the information reading unit receives a plurality of product codes related to different product information from the contactless communication tag and sequentially outputs the product codes to the output unit.

44. The portable tag reader of claim 27, further comprising an encryption unit that encrypts data to be transmitted to the contactless communication tag based on encryption key related information selected from the encryption key related information by encryption key specifying information received from the contactless communication tag.

45. The portable tag reader of claim 27, wherein area of the portable tag reader is the same as that of a credit card and thickness of the portable tag reader is similar to a thin-type battery.

46. A method of providing product information using a tag reader that communicates with a contactless communication tag attached to a product, the method comprising:

receiving encryption key specifying information from the contactless communication tag;

selecting encryption key related information corresponding to the received encryption key specifying information from encryption key related information stored in a storing means included in the tag reader;

transmitting an information request message that requests the product

information to the contactless communication tag;

reading the product information received from the contactless communication tag based on the selected encryption key related information; and

outputting a result of reading concerning the product information.

47. The method of claim 46, further comprising:

receiving encryption key update request information concerning a leaked encryption key from the contactless communication tag; and

removing an encryption key designated by the encryption key update request information from the storing means and updating with a newly assigned encryption key.

48. The method of claim 46, wherein the encryption key related information includes a plurality of encryption keys that is classified and assigned according to a classification reference including at least one of a type of industry, a manufacturer, a brand, and a product name; and

the decryption unit decrypts the product information received from the contactless communication tag using an encryption key selected from the plurality of encryption keys based on the encryption key specifying information received from the contactless communication tag.

49. The method of claim 46, wherein the encryption key related information includes at least one seed value for creation of different encryption keys; and

reading of the product information includes decrypting the product information received from the contactless communication tag using an encryption key using a seed value selected based on the encryption key specifying information received from the contactless communication tag.

50. The method of claim 49, further comprising:

receiving seed value update request information concerning a leaked seed value from the contactless communication tag; and

removing a seed value designated by the seed value update request information from the storing means and updating with a newly assigned seed value.

51. The method of claim 46, wherein the encryption key the encryption key related information includes a plurality of seed values that is classified and assigned according to a classification reference including at least one of a type of industry, a manufacturer, a brand, and a product name; and

reading of the product information includes decrypting the product information received from the contactless communication tag using an encryption key created based on a seed value selected from the plurality of seed values based on the encryption key specifying information received from the contactless communication tag.

52. The method of claim 46, further comprising receiving update request information concerning leaked encryption key related information from the contactless communication tag; and

removing encryption key related information designated by the update request information from the storing means and updating with newly assigned encryption key related information.

53. The method of claim 46, further comprising generating a one-time use random number, adding the one-time use random number to information to be transmitted to the tag reader, providing the information to the decryption unit, and checking if a random number extracted from information received from the tag reader is the same as the one-time use random number, thereby blocking replay attack.

54. The method of claim 46, wherein the storing means includes non-volatile memory and selection of the encryption key related information comprises:

selecting encryption key related information corresponding to the received encryption key specifying information from encryption key related information stored in the storing means included in the tag reader; and

reading the encryption key related information from the storing means and re-recording the read encryption key related information in the storing means.

55. The method of claim 46, wherein outputting of the result of reading

includes outputting a plurality of product information specified from a type of industry, a manufacturer, a brand, and a product name based on the encryption key specifying information received from the contactless communication tag.

56. The method of claim 46, further comprising:

authenticating an external portable tag reader by communicating with the external portable tag reader; and

outputting a result of authentication concerning the external portable tag reader.

57. The method of claim 46, wherein outputting of the result of reading includes receiving a plurality of product codes related to different product information and sequentially outputting the received product codes.

58. A product to which a contactless communication tag is attached, the contactless communication tag in which product information is stored, wherein the contactless communication tag comprises:

a contactless communication unit, which wirelessly exchanges data with a tag reader, creates a power source from a power signal received from the tag reader, and supplies the created power source;

a storing unit in which product information including genuineness information of the product and encryption key related information are stored;

an encryption unit, which encrypts a signal to be transmitted to the tag reader; and

an information providing unit, which reads the product information stored in the storing unit in response to a product information request message received from the tag reader and provides the read product information to the encryption unit,

wherein visible information corresponding to genuineness information of the product stored in the contactless communication tag is printed on or attached to the product.

59. The product of claim 58, wherein the genuineness information of the product and the visible information printed on or attached to the product are unique

codes that are assigned to the product.

60. The product of claim 58, wherein the genuineness information of the product is a color corresponding to the genuineness of the product, and the visible information printed on or attached to the product is a color corresponding to the genuineness of the product.

61. The product of claim 58, wherein the contactless communication tag is destroyed not to be accessed by the tag reader when the product is unsealed or the contactless communication tag is detached from the product by an external force.